**Amendments to the Claims:**

This listing of claims will replace all prior versions and listings of claims in the application.

**Listing of Claims:**

1. (Currently Amended) A system for providing quarantine on a network comprising:

a client device seeking access to a network resource, the client device configured to:

perform a first plurality of checks specified by a first manifest,

store a first status report at the client device, the first status report specifying results of the first plurality of checks, and

send a Bill of Health (BoH) request that contains the first status report;

a first server device that:

receives the BoH request sent by the client device,

determines whether the first status report indicates that the client device passed all of the checks specified by a second manifest that specifies a second plurality of checks that the client device must perform,

sends to the client device the second manifest when the first status report indicates that the client device did not pass all of the checks specified by the second manifest,

receives, from the client device, a second status report that indicates results of the client device performing the second plurality of checks,

stores a Bill of Health (BoH) for the client device when the second status report indicates that the client device passed all of the checks in the second plurality of checks, the BoH comprising a creation time of the BoH, an expiration date of the BoH, a manifest version identifier that identifies a version number of the second manifest, and an integrity check;

if the results of the second plurality of checks show that the client device

passed all of the checks in the second plurality of checks, sends, to the client device, a certificate that provides proof that the client device possesses a required configuration, the certificate comprising a serial number of the BoH, an address of the first server device, and a digital signature; and

a second server device that:

receives a request for access to the network resource from the client device, the request including the certificate,

uses the serial number in the certificate and the address of the first server device to retrieve the BoH from the first server device,

uses the digital signature of the certificate to determine whether any part of the certificate has been modified after the certificate was issued by the first server device,

after retrieving the BoH, uses the integrity check to determine whether the BoH has been tampered,

determines whether the expiration date of the BoH has passed,

determines whether the manifest version identifier identifies a most recent manifest version number,

provides access to the network resource when the second server device determines that the certificate has not been modified after the certificate was issued by the first server device, that the BoH has not been tampered, that the expiration date for the BoH has not passed, and that the manifest version identifier specifies the most recent manifest version number,

wherein the second server device denies the client device access to the network resource when the second ~~network~~ server device determines that the certificate has been modified after the certificate was issued by the first ~~quarantine~~ server device, that the BoH has been tampered, that the expiration date for the BoH has passed, or that the manifest version identifier does not identify the most recent manifest version number;

wherein the client device periodically requests that the certificate be updated by the first server device, regardless of whether the client device sends further requests for access to the network resource to the second server device.

2. (Previously Presented) The system of claim 1, wherein the second plurality of checks includes at least one of checks for: installed software, a software version, an installed patch, an installed anti-virus system, an anti-virus state, a firewall state, an installed service, file sharing, a registry value, a registry key, and a file system state.

3. (Previously Presented) The system of claim 1, wherein the client device comprises delegates that perform the checks in the first plurality of checks and the second plurality of checks.

4. (Previously Presented) The system of claim 1, wherein the client device stores a copy of the certificate in a database.

5. (Canceled)

6. (Canceled)

7. (Previously Presented) The system of claim 1, wherein if the client device cannot provide proof that the client device possesses the required configuration, the second server device directs the client device to the first server device.

8. (Canceled)

9. (Currently Amended) The system of claim 1, wherein the second server device includes a second database that is a replica of [[the]] a first database, wherein the client device proves possession of the required configuration by sending the second server device the serial number of the BoH, wherein the second server device compares the serial number of the BoH to a unique identifier stored with the certificate in the second database.

10. (Previously Presented) The system of claim 1, wherein the first server device

requests a software inventory from the client device and sends, to the client device, software necessary for the required configuration.

11. (Previously Presented) The system of claim 1, further comprising an access point for mediating communication between the client device and the second server device, wherein the second server device is protected by a firewall.

12. (Previously Presented) The system of claim 1, wherein the first server device and the second server device are one computing device.

13. (Currently Amended) A method for a client device to acquire access to a network resource, comprising:

performing, at the client device, a first plurality of checks specified by a first manifest;

storing a first status report at the client device, the first status report specifying results of the first plurality of checks;

sending a Bill of Health (BoH) request that contains the first status report from the client device to a first server device;

receiving, at the client device, a second manifest of checks from the first server device when the first server device determines that the first status report indicates that the client device did not pass all of the checks specified by the second manifest, wherein the checks of the second manifest determine whether the client device possesses a required configuration;

performing, at the client device, the checks in the second manifest of checks;

sending, from the client device to the first server device, a second status report that indicates results of the checks of the second manifest;

receiving, at the client device from the first server device, a certificate that provides proof that the client device possesses the required configuration,

wherein the certificate comprises a serial number of a BoH for the client device stored at the first server device, an address of the first server device, and a digital signature, and

wherein the BoH comprises a creation time of the BoH, an expiration date for the BoH, a manifest version identifier that identifies a version number of the second manifest, and an integrity check;

sending, from the client device to a second server device that controls access to the network resource, a request for access to the network resource;

sending, from the client device to the second server device, the certificate;

receiving, at the client device, access to the network resource when the certificate has not been modified after the certificate was issued by the first server device, the BoH has not been tampered, the expiration date for the BoH has not passed, and the manifest version identifier of the BoH identifies a most recent manifest version number;

periodically requesting, from the client device, that the certificate be updated by the first server device, regardless of whether the client device sends further requests for access to the network resource to the ~~network~~ second server device.

14. (Previously Presented) The method of claim 13, further comprising:

receiving, at the client device, a request for a software inventory from the first server device;

receiving, at the client device, software necessary for the required configuration; and

installing the software at the client device.

15.-17. (Canceled)

18. (Currently Amended) The method of claim 13, wherein the first server device and the second server device are one computing device.

19.-22. (Canceled)

23. (Currently Amended) A method for quarantining a client device from access to a network resource, comprising:

receiving, at a first server device, a request for access to the network resource

from the client device;

receiving, at the first server device from the client device, a certificate that provides proof that the client device has a required configuration, wherein the certificate specifies a serial number of a Bill of Health (BoH) generated by a trusted server device that only generates the BoH when the trusted server device receives, from the client device, a status report that indicates results of checks specified in a manifest sent to the client device by the trusted server device and the results of the checks show that the client device passed all the checks;

sending, from the first server device to the trusted server device, a request for the BoH, the request for the BoH specifying the serial number of the BoH;

receiving, at the first server device, the BoH, the BoH specifying a creation time of the BoH, an expiration date for the BoH, a manifest version identifier that specifies a version number of the manifest, and an integrity check;

validating, at the first server device, the certificate when the certificate has not been modified after the certificate was issued by the trusted server device, the BoH has not been tampered, the expiration date of the BoH has not passed, and the manifest version identifier specifies a most recent manifest version number;

if the certificate is valid, allowing the client device access to the network resource;

if the certificate is invalid, denying the client device access to the network resource; and

wherein the trusted server device periodically receives from the client device a request that the [[proof]] certificate be updated, regardless of further requests for access to the network resource.

24. (Previously Presented) The method of claim 23, further comprising, if the certificate is invalid, directing, at the first server device, the client device to the trusted server device so that the required configuration is obtained.

25.-27. (Canceled)

28. (Currently Amended) One or more computer readable storage media having computer-executable instructions that, when executed by a processing unit in [[the]] a client device, cause the client device to perform a method for [[a]] the client device to acquire access to a network resource, the method comprising the steps of:

performing, at the client device, a first plurality of checks specified by a first manifest;

storing a first status report at the client device, the first status report specifying results of the first plurality of checks;

sending a Bill of Health (BoH) request that contains the first status report from the client device to a first server device;

receiving, at the client device, a second manifest of checks from [[a]] the first server device when the first server device determines that the first status report indicates that the client device did not pass all of the checks specified by the second manifest, wherein the checks of the second manifest determine whether the client device possesses a required configuration of installed software;

performing, at the client device, the checks in the second manifest of checks;

sending a second status report that indicates results of the checks of the second manifest from the client device to the first server device;

receiving, at the client device from the first server device, a certificate that provides proof that the client device possesses the required configuration,

wherein the certificate comprises a serial number of a BoH for the client device stored at the first server device, an address of the first server device, and a digital signature, and

wherein the BoH comprises a creation time of the BoH, an expiration date for the BoH, a manifest version identifier that identifies a version number of the second manifest, and an integrity check;

sending, from the client device to a second server device that controls access to the network resource, a request to access to the network resource;

sending, from the client device to the second server device, the certificate;

receiving, at the client device, access to the network resource when the certificate has not been modified after the certificate was issued by the first server device, the BoH

has not been tampered, the expiration date for the BoH has not passed, and the manifest version identifier of the BoH identifies a most recent manifest version number; and

periodically sending, from the client device to the first server device, a request to update the certificate [[proof]], regardless of further requests for access to the network resource.

29. (Currently Amended) A system for a client device to acquire access to a network resource, comprising:

a processing unit; and

a memory coupled with and readable by the processing unit and having stored therein instructions which, when executed by the processing unit, cause a module to perform the following acts:

performing, at the client device, a first plurality of checks specified by a first manifest;

storing a first status report at the client device, the first status report specifying results of the first plurality of checks;

sending a Bill of Health (BoH) request that contains the first status report from the client device to a first server device;

receiving, at the client device, a second manifest of checks from [[a]] the first server device when the first server device determines that the first status report indicates that the client device did not pass all of the checks specified by the second manifest, wherein the checks of the second manifest determine whether the client device possesses a required configuration;

performing, at the client device, the checks in the second manifest of checks;

sending, from the client device to the first server device, a second status report that indicates results of the checks of the second manifest;

receiving, at the client device from the first server device, a certificate that provides proof that the client device possesses the required configuration,

wherein the certificate comprises a serial number of a BoH for the client device stored at the first server device, an address of the first server

device, and a digital signature, and

wherein the BoH comprises a creation time of the BoH, an expiration date for the BoH, a manifest version identifier that identifies a version number of the second manifest, and an integrity check;

storing the certificate at the client device;

sending, from the client device to a second server device that controls access to the network resource, a request to access the network resource;

determining, at the client device, whether the certificate stored at the client device is valid;

sending, from the client device to the first server device, a request to update the proof if the certificate is no longer valid;

sending, from the client device to the second server device, the certificate of the required configuration; and

periodically sending, from the client device to the first server device, requests to update the certificate, regardless of further requests for access to the network resource.